Legislative Audit Division

State of Montana

Report to the Legislature

November 1995

EDP Audit Report

Information Processing Facility and Central Applications

Each year the Office of the Legislative Auditor audits the state's central computer facility and centralized computer applications. This report is used by financial-compliance and performance auditors and contains our conclusions and/or recommendations for improving general controls over the mainframe computer (Information Processing Facility) and application controls over the following systems:

▶ State Payroll System

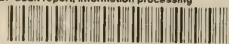▶ Statewide Budgeting and Accounting System

▶ Warrant Writer System

Direct comments/inquiries to:
Legislative Audit Division
Room 135, State Capitol
PO Box 201705
Helena Montana 59620-1705

95DP-33

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Legislative Audit Division are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

November 1995

The Legislative Audit Committee
of the Montana State Legislature:

     This is our EDP audit of controls relating to the state's centralized data processing systems operated by the Department of Administration and the State Auditor's Office. We reviewed the Department of Administration's general controls over the Information Processing Facility and application controls over State Payroll and the Statewide Budgeting and Accounting System (SBAS). In addition, we reviewed application controls over the Warrant Writer system, operated by the State Auditor's Office during fiscal year 1994-95. This report contains recommendations for improving EDP controls related to SBAS, State Payroll, and Warrant Writer systems and the Information Processing Facility. Written responses to our audit recommendations are included in the back of the report.

     We thank the Department of Administration and State Auditor's Office for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Information Processing Facility and Central Applications

Table of Contents

Appointed and Administrative Officials

Department of
Administration

Lois Menzies, Director

Connie Griffith, Administrator
Accounting and Management Support Division

Terry Atwood, Chief
Accounting Bureau

Tony Herbert, Administrator
Information Services Division

Jeff Brandt, Chief
Policy, Development, and Customer Relations Bureau

Paul Rylander, Chief
Computing Operations Bureau

Mark Cress, Administrator
Personnel Division

John McEwen, Chief
Classification and Pay Bureau

Donna F. Warner, Supervisor
State Payroll

Introduction

This EDP Audit reviewed centralized controls over the state's mainframe computer and the State Payroll, the Statewide Budgeting and Accounting System (SBAS), and the Warrant Writer computer based applications. The audit included a general control review of the state's mainframe computer and application reviews of State Payroll, SBAS, and Warrant Writer. A discussion of general and application controls is included on pages 1 and 2. The audit objectives and scope are discussed on pages 2 and 3 of the report.

General Controls

The Department of Administration's Information Services Division (ISD), provides mainframe data processing services to state agencies. Processing is performed on an IBM computer operating 24 hours a day except during scheduled system maintenance. Between 8:00 a.m. and 5:00 p.m. the central computer operates at 90 percent operating capacity.

General controls are developed by management to ensure computer operations function as intended and provide effective data processing service to users. Except as noted below, the department's general control environment provides for controlled application processing on the mainframe computer system. Additional discussion of the audit issues is included in Chapter II.

Physical Access to Operating System Documentation

Operating system documentation includes installation guidelines and procedures, system configurations, user-written modifications, software installation programs, etc. In our previous audit we recommended the department restrict access to operating system documentation to only those employees who require access to perform job duties.

The department has not implemented our prior recommendation but indicated they intend to install a file cabinet to secure selected system documentation. Unrestricted access could allow unauthorized individuals to change operating system specifications or destroy installation documentation. ISD should secure operating system documentation, including installation guidelines and procedures manuals, in locked storage cabinets.

Report Summary

Physical Inventory of Data Cartridges at Storage Facility

Twice each week, ISD employees back-up all mainframe operating system software, application programs, and data to magnetic tape cartridges, which they store at an off-site facility. In our previous audit we recommended the department complete and document a formal annual inventory of back-up data stored at the off-site storage facility. During the current review ISD personnel indicated they completed but did not document an inventory.

Documented inventory procedures will support subsequent inventory records and assist backup personnel in completing inventory duties. Without documentation, the department cannot ensure electronic records agree to the existing data cartridge inventory.

Authorization for Transferring or Deleting Agency Data Cartridges

Department personnel transfer data cartridges at the Information Processing Facility data center to and from the off-site storage area per agency request. Although department procedure requires documented agency authorization, employees periodically transfer or delete agency data files upon verbal request.

EDP guidelines suggest management establish physical security procedures to safeguard electronic data from loss or unauthorized access. Documented authorization can support additions or deletions to inventory records and ensure department personnel complete requests as intended.

Application Controls

The audit reviewed application controls over SBAS, State Payroll, and Warrant Writer. SBAS is an accounting system which provides financial reporting of agency transactions. State Payroll processes payroll for state agencies and selected units of the Montana University System. Warrant Writer creates state warrants from agency submitted transfer warrant claims processed through SBAS. As discussed in Chapter III, application controls were effective and adequate to ensure accurate and complete data processing for SBAS, State Payroll, and Warrant Writer.

Introduction

This is our annual electronic data processing (EDP) audit of the state's centralized data processing systems. The audit included centralized controls over the state's mainframe computer and three computer based applications: State Payroll, Warrant Writer, and the Statewide Budgeting and Accounting System (SBAS).

The audit was at the Department of Administration which maintains the state's mainframe, State Payroll, and SBAS. The audit also included work at the State Auditor's Office which had primary responsibility for Warrant Writer. Effective July 1, 1995, administrative responsibility for the Warrant Writer application transferred from the State Auditor's Office to the Department of Administration. The controls identified and tested are relied upon by financial-compliance, performance, and EDP audits covering fiscal year 1994-95.

Organization of Report

The report contains three chapters. Chapter I contains the introduction, background information, and audit objectives. Chapter II discusses our review of general controls applicable to the Department of Administration's Information Processing Facility. Chapter III includes our application review of the department's SBAS, State Payroll, and Warrant Writer mainframe computer applications.

EDP Audit General and Application Controls

EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. A general control review includes an examination of the following controls:

Organizational - apply to the structure and management of the computing and information services facility. Specific types of organization controls include segregation of duties, assignment of responsibilities, rotation of duties, and supervision.

Procedural - operating standards and procedures which ensure the reliability of computer processing results and protect against processing errors.

Hardware and Software - controls within the operating system software and hardware which monitor and report system error conditions.

System Development - oversight and supervisory controls imposed on development projects. Controls include feasibility studies, development, testing and implementation, documentation, and maintenance.

Physical Security - physical site controls including security over access to the computer facility, protection devices such as smoke alarms and sprinkler systems, and disaster prevention and recovery plans.

Electronic Access - controls which allow or disallow user access to electronically stored information such as data files and application programs.

A general control review provides information regarding the ability to control EDP applications. Application controls are specific to a given application or set of programs that accomplish a specific objective. Application controls consist of an examination of the following controls and objectives:

Input - Ensure all data is properly coded to machine language, all entered data is approved, and all approved data is entered.

Processing - Ensure all data input is processed as intended.

Output - All processed data is reported and properly distributed to authorized individuals.

A review of the application documentation and audit trail is also performed. Applications must operate within the general control environment in order for reliance to be placed on them.

Audit Objectives

The objectives of this EDP audit were to determine the adequacy of:

1. General controls specific to the state mainframe computer.

2. Application controls over data processed by the SBAS, State Payroll, and Warrant Writer applications.

**Audit Scope and
Methodology**

The audit was conducted in accordance with government audit
standards. We compared existing general and application controls
against criteria established by the American Institute of Certified
Public Accountants (AICPA), United States General Accounting
Office (GAO), and the EDP industry.

We reviewed the Department of Administration's general controls
related to the state mainframe environment. We interviewed
department personnel to gain an understanding of the hardware and
software environment at the Department of Administration. We
also examined documentation to supplement and confirm
information obtained through interviews.

We examined procedures within the mainframe environment which
ensure computer processing activities are controlled. For example,
we determined if mainframe equipment is maintained in a secured
area and access is limited to authorized personnel. The department
provides data entry and processing services to state agencies. We
reviewed department procedures which ensure data processing is
completed per agency authorization.

We conducted application reviews over State Payroll, Warrant
Writer, and SBAS. We interviewed employees of the Department
of Administration and the State Auditor's Office to evaluate
policies and procedures. We reviewed input, processing, and
output controls for these systems. We also reviewed supporting
documentation to determine if controls over data are effective as
well as adequate to ensure the accuracy of data during processing
phases.

Controls over centralized operations are supplemented by controls
established at user agencies. We did not review controls
established by user agencies.

Compliance

We determined compliance with applicable state laws and rules and Montana Operations Manual policies. Except as discussed on page six, we found the Department of Administration and the State Auditor's Office to be in compliance with applicable laws, rules, and state policy.

Prior Audit Recommendations

Our prior audit report for fiscal year 1993-94 included eight recommendations still applicable to the Department of Administration. The department concurred with each recommendation. As noted below, the department implemented four recommendations, partially implemented two recommendations, and did not implement two recommendations.

The two recommendations not implemented concern physical security of operating system documentation and inventory controls over data storage. These issues are discussed on pages seven and nine of this report. The previous recommendation concerning disaster recovery, which the department has partially implemented, is discussed on page six.

The department partially implemented our recommendation to State Payroll. Previously, we recommended the department obtain documented agency authorization for adjustments made to processed payroll transactions. We found the department established and implemented corrective procedures following supplemental consultation with Audit Division staff. Therefore, we make no further recommendation at this time.

Chapter II - General Controls

Introduction

The department's Information Processing Facility (IPF) is located in the basement of the Mitchell Building in Helena. State employees process application programs and data stored on the mainframe through personal computers and terminals located across the state. This chapter discusses our review of management's operating procedures and controls which ensure continuous, reliable, and accurate mainframe data processing services.

Information Processing Facility

The Department of Administration's Information Services Division (ISD), provides data processing services for use by state agencies. Central data processing services include: central mainframe computer processing; design, development, and maintenance support of data processing applications; and disaster recovery facilities for critical data processing applications. Processing is performed on an IBM computer operating 24 hours a day except during scheduled system maintenance. Between 8:00 a.m. and 5:00 p.m. the central computer operates at 90 percent operating capacity.

Conclusion: General controls provide controlled application processing

General controls are developed by management to ensure computer operations function as intended and provide effective data processing service to users. Except as noted below, we determined the department's general control environment provides for controlled application processing on the mainframe computer system.

Physical Security

Physical security controls provide security against accidental loss or destruction of data and program files or equipment and ensure continuous operation of EDP functions. Physical security controls include: safeguard of files, programs and documentation; physical access over the computer facility; and a plan or method to ensure continuity of operations following major destruction of files or hardware breakdown.

We reviewed existing physical controls in place at the Information Processing Facility. The department maintains computer hardware on a raised floor. Smoke alarms function properly. Air

conditioning maintains controlled computer room temperature. The power supply meets computing equipment needs. The following sections discuss areas where we believe the department could improve physical security controls.

ISD Improves Disaster Recovery Preparedness - State Agencies Should Follow

The Department of Administration received funding from the 1991 Legislature to adequately design and implement a contingency plan, which included a "hotsite" and the appropriate backup equipment. In February 1992, ISD established a five year contract for a backup hotsite with Weyerhaeuser Information Systems in Federal Way, Washington. The hotsite agreement provides ISD an alternative location and equipment necessary to recover mainframe computer operations. The contract also provides for annual on-site recovery testing of the central mainframe operating system and agency-owned applications such as State Payroll and the Statewide Budgeting and Accounting System (SBAS).

Each year we review the status of ISD's disaster recovery plan. Previously we recommended the department complete and document a formal recovery plan. During fiscal year 1994-95 ISD documented, in draft form, a recovery plan which defines ISD personnel responsibilities, hardware and software requirements, and mainframe operating system recovery procedures. During the next fiscal year, ISD plans to finalize and test the recovery plan. Once finalized, the plan will help ensure ISD's efficient recovery following a disaster.

We also recommended the department request agency participation and provide assistance to state agencies for development of application recovery procedures. After completing its recovery plan, ISD intends to provide guidance to state agencies for documenting agency application recovery procedures within the plan. In November 1994, ISD included selected state agency applications in its annual recovery test process. Through coordination with application owners, ISD recovered the State Payroll, Warrant Writer, and SBAS applications. This allowed the application users to perform processing tests at the hotsite from computer terminals in Helena.

Based on our review of ISD's progress in disaster recovery, we found ISD has partially implemented both parts of our previous recommendation. We continue to have concerns regarding state agency participation in disaster recovery procedures. In previous audits at state agencies, we have found state agencies assume ISD will automatically recover their mainframe applications. Although ISD can recover agency applications and provide mainframe connection capabilities for agency-owned terminals, ISD cannot define agency application recovery priorities or personnel responsibilities. In addition, state agencies must coordinate recovery testing with ISD to verify recovery procedures are reliable.

Disaster recovery planning requires ongoing preparation. By establishing documented procedures, ISD significantly improved its ability to recover mainframe computing operations following a disaster. We will continue to review the status of ISD's disaster recovery plan and make no further recommendation at this time. We also continue to review state agency disaster recovery procedures during financial-compliance, performance, and EDP audits.

Physical Access to Operating System Documentation

Operating system documentation includes installation guidelines and procedures, system configurations, user-written modifications, software installation programs, etc. ISD's Operating System Support programmers refer to system documentation daily and during periodic modifications or installations of operating system software. For example, when performing software installations, operating system programmers document installation procedures and system specifications.

In our previous audit we recommended the department restrict access to operating system documentation to only those employees who require access to perform job duties. ISD had remodeled office space and, as a result, access to the system documentation was no longer restricted during non-working hours.

During our current review department personnel indicated they plan to install a file cabinet to secure selected system documentation. We believe all system documentation, including installation

guidelines and procedures, should be secure from unauthorized access.

EDP guidelines suggest management restrict access to operating system documentation to individuals who require access to perform job duties. Unrestricted access could allow unauthorized individuals to change operating system specifications or destroy installation documentation. ISD should secure operating system documentation, including installation guidelines and procedures manuals, in locked storage cabinets.

Recommendation #1

We recommend the department restrict access to operating system documentation to those employees who require access to perform job duties.

Physical Security of Data Cartridges

Data cartridges provide magnetic storage for electronic data, system software, and application programs. The department creates and stores data cartridges at the Information Processing Facility computer center. Cartridges having a long-term retention date and those used for back-up are stored at an off-site facility.

A librarian function provides physical security over mainframe back-up software and data cartridges by verifying cartridge location and ensuring only authorized individuals are permitted to remove cartridges from the library. Department personnel use an electronic tape management system, which utilizes bar code technology similar to grocery store checkout stands, to track cartridge movement between the central facility and off-site storage location.

We reviewed department procedures for maintaining custody over data cartridges located in the data center and the off-site facility. The following sections discuss our recommendations for improving physical security controls over data cartridges.

Physical Inventory of Data Cartridges at Storage Facility

Twice each week, ISD employees back-up all mainframe operating system software, application programs, and data to magnetic tape cartridges, which they store at an off-site facility. In our previous audit we recommended the department complete and document a formal annual inventory of back-up data stored at the off-site storage facility. During our current review ISD personnel indicated they completed an inventory of magnetic data cartridges at the data center and the off-site facility. However, we were unable to verify an inventory was completed or evaluate the inventory procedures because personnel did not formally document the review.

EDP guidelines suggest management perform an annual physical inventory to verify assets and ensure accuracy of inventory records. A complete physical inventory provides management the ability to verify backup data location and existence. Without a complete inventory, ISD may be unable to locate critical data following a disaster.

ISD employees use an electronic tape management system to identify and document back-up tape location. The electronic system should enable ISD employees to efficiently complete an annual physical inventory of magnetic tape cartridges stored at the data center and off-site facility. In addition, documented inventory procedures will support subsequent inventory records and assist backup personnel in completing inventory duties. Without documentation, the department cannot ensure electronic records agree to the existing data cartridge inventory.

Recommendation #2

We recommend the department document a formal annual inventory of back-up data stored at the off-site storage facility.

Authorization for Transferring or Deleting Agency Data Cartridges

In addition to maintaining custody over magnetic tape cartridges librarian procedures include daily accounting for tape inventory additions and deletions. Department personnel transfer data cartridges at the Information Processing Facility data center to and from the off-site storage area per agency request. The department has established a procedure for transferring or deleting agency data files upon documented agency request, but employees do not consistently follow the procedure. Employees transfer or delete library tapes upon verbal agency request.

EDP guidelines suggest management establish physical security procedures to safeguard electronic data from loss or unauthorized access. Documented authorization can support additions or deletions to inventory records and ensure department personnel complete requests as intended. Department employees indicated they do not require documented agency authorization if they recognize the individual requestor.

Recommendation #3

We recommend the department obtain documented agency authorization for transferring or deleting agency data cartridges from the tape library.

Chapter III - Application Controls

Introduction

We reviewed application controls over the Statewide Budgeting and Accounting System (SBAS) and State Payroll as operated by the Department of Administration.

We also reviewed application controls over the Warrant Writer system, operated by the State Auditor's Office during fiscal year 1994-95. Effective July 1, 1995 administrative responsibility for Warrant Writer transferred to the Department of Administration. Therefore, we address related audit recommendations to the Department of Administration.

Statewide Budgeting and Accounting System

The Department of Administration's Accounting Bureau operates the Statewide Budgeting and Accounting System. SBAS is an accounting system which provides financial information used to review and control agency financial transactions. The system also provides agency management budgetary control data used for decision making. SBAS provides uniform accounting and reporting for all state agencies by showing receipt, use, and disposition of all public money and property in accordance with generally accepted accounting principles (GAAP).

State agencies input SBAS documents using On-line Entry & Edit (OE&E) or submit transactions to the OE&E database by remote job entry. The input documents are held in a processing queue until Accounting Bureau runs a nightly job which gathers the data. SBAS edits check the data to ensure validity. If a document does not pass through the edits, it will reject from SBAS and may require correction. Documents which pass SBAS edits are processed and posted to the SBAS database. SBAS is a combination of on-line entry and batch update.

Conclusion: SBAS application controls effective and adequate for fiscal year 1994-95

We performed an application review of SBAS. We determined input, processing, and output controls over SBAS were effective, as well as adequate, to ensure data integrity during processing phases for fiscal year 1994-95.

State Payroll System

The State Payroll System, operated by Department of Administration, processes payroll for state agencies and selected units of the Montana University System. The State Payroll System is also referred to as the Payroll/Personnel/Position Control system (P/P/P). The payroll component issues and tracks state of Montana employees' wage and benefit payments. The payroll component also calculates payroll deductions, leave and service adjustments, automatic salary increases, and direct bank deposits upon request. The personnel component records detailed information about each state employee such as birth, sex, disability, and emergency notification for each employee. The personnel database also includes information to verify compliance with state and federal labor laws. The position control component provides management with information necessary for budgeting purposes and includes information on employee position number, grade, classification code, date of hire, and longevity.

Conclusion: State Payroll application controls effective and adequate for fiscal year 1994-95

Our EDP audit was limited to application controls applicable to payroll transactions processed through the State Payroll System. We determined input, processing, and output controls over the State Payroll System were effective as well as adequate, to ensure payroll data integrity during processing phases for fiscal year 1994-95.

Warrant Writer System

The Warrant Writer system controls creation and distribution of most state warrants and the redemption of all state warrants. The system creates state warrants from agency submitted transfer warrant claims processed through SBAS. Every week-night, after SBAS is updated with the daily transactions, a SBAS report identifies the warrants to be written the following morning. The system accounts for state warrants issued, outstanding, and redeemed.

Effective July 1, 1995 the responsibility for the Warrant Writer system transferred to the Department of Administration. During fiscal year 1994-95 the State Auditor's Office and the Department of Administration jointly operated and maintained Warrant Writer. However, the State Auditor's Office was primarily responsible for the system. Department of Administration initiated warrant writing

and reconciled issued warrants to SBAS. The State Auditor's Office prepared warrants, distributed warrants, and reconciled warrants outstanding to SBAS. Both agencies jointly controlled warrant redemption.

Conclusion: Warrant Writer application controls effective and adequate for fiscal year 1994-95

We performed an application review of the Warrant Writer system. We determined input, processing, and output controls over Warrant Writer were effective, as well as adequate, to ensure data integrity during processing phases for fiscal year 1994-95. As discussed below, the department should consider a system modification to the Bad Debts component of Warrant Writer to offset direct deposits.

Offsets should be Established for Direct Deposits

The Bad Debts component of the Warrant Writer system withholds warrants written to the payee if that payee owes money to the state of Montana. During warrant processing, an electronic file of debtors is compared against warrant payees. If a match is identified, department personnel adjust or "offset" the warrant for the amount owed to the state of Montana. We found the Bad Debt system is unable to automatically offset state of Montana payments made by direct deposit.

Section 17-4-105(2), MCA, requires the Department of Administration to offset any amount due from the payee to the state of Montana. Although state law does not specifically address direct deposits we believe the department should modify system programming to provide for a direct deposit offset.

Department employees manually offset approximately 300 direct deposit payments each month. This procedure requires employees adjust daily direct deposits and issue state warrants for any balance remaining following offset. They expect this figure to increase in relation to a growing trend toward payment by direct deposit. For example, state income tax refunds will be available by direct deposit upon taxpayer request. In addition, state agencies currently pay fifty-six cents per mailed warrant or sixteen cents for each direct deposit. Department employees believe this savings will encourage state agencies to pay their vendors by direct deposit. The cost to automate the direct deposit offset process can be recovered by enabling employees to more effectively process bad debt adjustments.

Recommendation #4

We recommend the department modify the Warrant Writer system to provide for automatic offsets against direct deposits.

Agency Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

MARC RACICOT, GOVERNOR
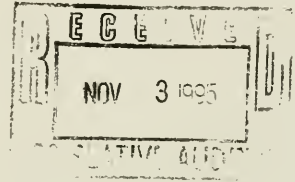
MITCHELL BUILDING

— STATE OF MONTANA —

(406) 444-2032
FAX: 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

November 2, 1995

Scott A. Seacat
Legislative Audit Division
State Capitol
Helena, MT   59620

Dear Scott:

We have reviewed the recommendations in the Information Processing Facility and Central Applications EDP Audit dated November 1995. Our responses follow:

Recommendation #1: We recommend the department restrict access to operating system documentation to those employees who require access to perform job duties.

Response: We concur. The department will purchase a locking cabinet to store all critical system documentation and require personnel to file all documentation upon their daily departure.

Recommendation #2: We recommend the department document a formal annual inventory of backup data stored at the off-site storage facility.

Response: We concur. This procedure has already been established within ISD. However, this year the documentation was inadvertently discarded. When performing future inventories, we will adhere more closely to the procedure.

Recommendation #3: We recommend the department obtain documented agency authorization for transferring or deleting agency data cartridges from the tape library.

Response: We concur. It is ISD's policy to require a written authorization for tape data sets to be released before their established release date. This policy is closely followed. The only regular "transferring" of tapes is from the tape library to the off-site vault and back to the tape library. Any tape data sets that the user must send to a remote location are written to a separate pool of tapes set up for that
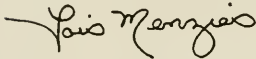
Page B-3

specific purpose, alleviating the need to remove any cartridges from our regular tape library.

Recommendation #4: **We recommend the department modify the Warrant Writer system to provide for automatic offsets against direct deposits.**

Response: We concur. We will program the pre-warrant processing job so that direct deposit warrants are automatically run through the offset process. However, if there is an offset to a direct deposit warrant, any remaining amount must be released as a regular warrant. To pay any released amount as a direct deposit will require major reprogramming of the pre-warrant processing job, which is not cost effective at this time. This change will be considered and incorporated in future rewrites of the Warrant Writer system.

We appreciate the opportunity to work with your staff on these issues.

Sincerely,

LOIS MENZIES
Director